Department of Commerce
Docket No. 100402174-0238-02 RIN 0660-XA12
Information Privacy and Innovation in the Internet Economy
Notice of Inquiry Comments
14 June 2010

I. Introduction

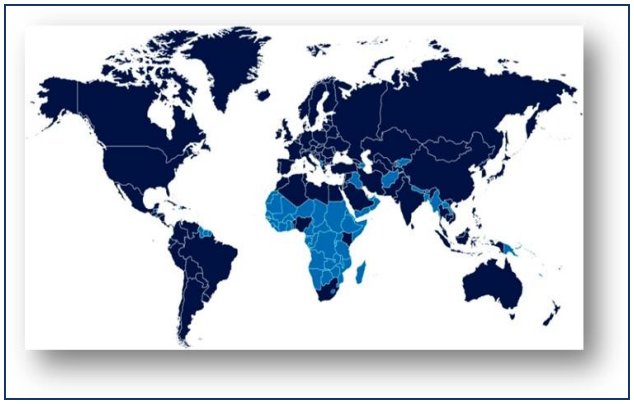
GS1 US is a not-for-profit organization established over 35 years ago to administer and manage Universal Product Codes, also known as U.P.C.'s. Since then, our membership and mission have expanded considerably.

Our method of identifying products and capturing product data has evolved into what is now known as the GS1 System, the world's most widely used supply chain standards, which include:

- a sophisticated array of numbering formats (identification numbers) for **identifying** different objects;
- a variety of bar codes and the Electronic Product Code (EPC), for **capturing** the identifying numbers; and
- data synchronization and electronic information exchange, for **sharing** the data.

GS1 US member companies represent more than 200,000 American businesses in more than 20 industries including consumer packaged goods, apparel, government, aerospace, retail, foodservice, healthcare, fresh and packaged foods, consumer electronics and high-tech. Some of the world's largest corporations participate in our boards and work groups, motivated by the knowledge that GS1 standards help their companies reduce costs and increase both the visibility and security of their supply chains.

GS1 US is one of 108 country-based Member Organizations of GS1. GS1 is a global organization dedicated to the development of standards and solutions to improve the efficiency and visibility of supply and demand chains, both globally and across industries. More than one million companies use GS1 standards to do business across 150 countries. GS1 and its subsidiaries and partnerships connect companies with standards-based solutions that are open, consensus-based, and universally endorsed.



GS1 US is <u>not</u>:

- a software provider
- a hardware provider
- a commercial solutions provider
- a technology company
- a trade organization
- a government agency

GS1 plays a proactive role in standards development by supporting research at leading academic laboratories around the world. Its Electronic Product Code was the result of such research as well as the work of several hundred companies represented in what became the second largest consortium at MIT, trailing only the World Wide Web Consortium.

GS1 knows firsthand the difficulties in developing and introducing new technologies. Few people now remember the swirl of controversy that surrounded the introduction of the now ubiquitous bar code in retail settings. Opponents of the use of bar codes warned of dire consequences for consumers and sought to prevent the use and deployment of bar codes; today it is hard to imagine losing the benefits of bar codes such as faster checkouts and the lower prices enabled by improved supply chain management.

Controversies such as those involving the introduction of bar codes have helped GS1 to understand the importance of broadly inclusive processes in developing appropriate policies. With that in mind, we commend the Department of Commerce, and other government agencies such as the FTC and the FCC for their expansive efforts to involve the public in important policy reviews. We support the view, expressed in the NOI, that recent technological developments, new applications, changing attitudes and expectations of privacy along with the growth of global connectivity make it timely to review existing privacy policies to ensure they meet the needs of the 21st century. GS1 is committed to participating in this process and pleased to provide its views on this important topic.

II. Key Considerations in Developing Policy

The core mission of GS1 is to create and implement standards and policies that will facilitate the growth of global commerce. We firmly support the global flow of information. But we realize that commerce cannot thrive in an environment where there is no effective fabric of trust and where consumers do not participate because they lack confidence that they will be fairly treated and that their personal information will be appropriately protected.

Therefore we fully subscribe to the goals which the Department has set out for privacy policies: that they will enhance: "[1] the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy; [2] the public confidence necessary for full citizen participation with the Internet; and [3] uphold fundamental democratic values essential to the functioning of a free market and a free society."

Given our global presence and the experience of our members, we would like to highlight several considerations:

- It is becoming increasingly important to develop policies while considering the global context and the need to harmonize policies to the extent possible consistent with fundamental values;

- Information is the lifeblood of commerce. Any restrictions must consider and reflect the benefits that will be foregone as well as the potential harms they are designed to avoid. We do not mean to imply that there are not justifiable restrictions, but the policy goal should be to find an appropriate balance between sometimes conflicting values. In determining that balance, policymakers should recognize the importance of the free flow of information for economic, social and political reasons;

- It is critical for policymakers to take a long view. The success of Privacy Guidelines issued by OECD and APEC is based in part on the focus on lasting principles applicable in a wide variety of circumstances. Lasting policies are based on careful analysis, not anecdote or headline;

- Electronic commerce has the potential to improve the living conditions of people around the world. But progress depends on our capacity to innovate. Without innovation, there is little chance that the next generation will inherit a better world.

Given its global view and its role in supporting innovation and commerce, we are pleased that the Department of Commerce has taken a leading role in this review of privacy policy.

III. Self Regulation

Too many policy debates pit proponents of new laws and regulations against advocates for self-regulation as if policy makers need to choose one path or another, embracing regulation and legislation or leaving the field open for private parties to make choices unencumbered by governmental action. This is not the real choice faced by policymakers. The real issue is determining the appropriate mix of these policy tools, which requires analysis, rather than sloganeering. Policymakers have recognized that mixed systems of laws and regulation combined with self-regulation can provide more efficient and effective means of achieving policy goals. This has been true in the realm of privacy policy in the U.S. for many years as well as in other areas where there are important competing interests that need to be appropriately weighed.

In determining the appropriate mix of policy tools, we do believe there are important needs served by clear and well-crafted laws and regulations. They can and should reflect lasting and publicly supported principles and provide clarity in the "rules of the road". They should establish boundaries while maximizing the ability of private parties to innovate and to make decisions based on their unique circumstances.

But we also believe strongly in the potential for self-regulation within the boundaries set by law. As laws and regulations become more and more detailed they become harder and harder to know, to understand, to obey, and to enforce. They inevitably leave gaps—inevitably because the world is constantly changing. But to the extent that laws set clear boundaries and reflect established principles, they can be complemented by effective self-regulation. Self-regulation has some clear advantages over ever more detailed legal dictates:

- Because "one-size fits all" policies often fail to meet their objectives because of the wide variation among those subject to the policies, it would be in the interest of policymakers to be able to "customize" policies. But laws and regulations are not designed for customization. Those subject to rules are the most knowledgeable parties about their internal plans and procedures and can structure them appropriately to accomplish policy goals;

- Those subject to the rules have the strongest incentives to find the most efficient and effective means of accomplishing policy goals;

- Self-regulation encourages innovation by the entities subject to it rather than simply turning over decisions to governmental entities. As the open standards movement demonstrates, there are substantial advantages in defining standards while encouraging innovation on top of those standards. Similarly, the open source movement demonstrates the value of recognizing the contributions that come from the widest possible range of sources;

- By encouraging those subject to policies to take responsibility through self-regulation, policymakers can focus on setting boundaries, overseeing behaviors, and enforcing those laws and regulations which set boundaries and which are not as amenable to self-regulatory regimes.

Self-regulation is consistent with the basic principles of devolution, attempting to drive decisions down to the lowest possible level because of the value of localized expertise and the strong incentives for effectiveness and efficiency that can be found at the local level. We would encourage the Department to recognize the utility of self-regulation and to incorporate it as a vital part of the privacy framework.

IV. A Recent and Ongoing Study in Government – Industry Cooperation for Principles-based Self Regulation

Over the last several years, GS1 has been working with the European Commission on a largely self-regulatory project to create a Framework for privacy impact assessments (PIAs) to help enterprises evaluate new radio frequency identification (RFID) applications. The Framework initiative has occurred under the umbrella of the European Union's *Directive on Data Protection* and the *European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification.* While the process of developing and implementing the PIA Framework is not yet complete, it has provided a number of useful lessons about the importance of government – industry cooperation, the role of self-regulation within a larger legal context, and the benefits of a principle-based approach:

`

Government – industry cooperation

- The process benefited from a willingness of various industry sectors to work together to create a PIA Framework of general applicability and one that could be customized to meet the needs of a particular industry sector. The consultative process that was established to create the PIA Framework was a broadly inclusive one involving non-governmental entities, academics etc., all of whom provided valuable feedback;

- The process for developing the PIA Framework also involved feedback from the data protection officials from the various countries of the European Union operating through the Article 29 Committee.

Principles-based approach

- The PIA Framework establishes guidelines for PIAs that address the full range of privacy principles, including notice, choice, responsible uses, data sharing, accountability, and others;

- The process encourages building in privacy protections in applications (privacy by design) rather than having privacy measures bolted on to applications after their implementation.

Self regulation

- The draft PIA process establishes appropriate internal review and approval procedures and processes for new RFID applications, involving not only operational personnel responsible for initiating the proposed application but also other appropriate management personnel;

- The process incents enterprises to become more self aware and conscious of privacy issues that might arise and to make more educated determinations on how they might be addressed.

The process has also confirmed a potential tension that is recognized in the NOI when multiple jurisdictions have different policies for the same activity. It is possible that a company proposing a new RFID application might have to submit its PIA for that application to dozens of different authorities throughout Europe for review. This could create unnecessarily duplicative work for the

entity submitting the PIAs as well as for the data protection authorities. Such burdens are disproportionately felt by small and medium-size enterprises (SMEs).

But even more potentially damaging would be conflicting rulings from various national authorities based on differences in national law making it difficult if not impossible for the petitioning company to operate centralized applications and to act, as is increasingly required, on a global basis.

V. Inconsistent or Conflicting Privacy Frameworks Create Barriers to Innovation and Deployment of New Technologies

In Section 2 of the Notice, the Department addressed the issue of the impact of diversity in state privacy policies. GS1 US has considerable experience in this area and is convinced that any potential gain in privacy protection in any single state jurisdiction is outweighed by the negative impacts of increased compliance costs, barriers to technology development and deployment, and increased customer confusion, particularly when state laws are technology specific.

GS1 Member Organizations work with members from over a hundred countries with vastly different legal and regulatory regimes. Yet an increasing number of our members offer goods and services globally and require the development of standards and systems that will work both locally and globally. These standards and systems are often subject to review and approval at many levels of government— for example local, state and national in the U.S., sub-national and national in Europe and Asia, and European-wide in Europe.

Inconsistent or conflicting privacy frameworks raise the cost of compliance which ultimately affects prices to consumers. But in some cases, inconsistent or conflicting rulings can actually make the development and deployment of new technology impossible. This can happen, for instance, if a local jurisdiction passes legislation that restricts or prohibits the use of a technology, or places inordinate burdens on it that cannot economically be met.

We strongly favor privacy policies that are technology neutral. New technologies entering the market already must overcome many obstacles, including the incumbent technologies they seek to replace. Handicapping new technologies with policies that burden them and are not applied to existing technologies may prove too much of a barrier to overcome, and, in any case discourage investment and deployment. Furthermore, technology specific policies may become obsolete overnight as new technologies arise.

Legislation recently considered in one state in the U.S. would have created a legal requirement that notices be provided to consumers about the use of RFID technology. We believe that notice is, and should remain a critical element of privacy frameworks and have included a notice requirement in the EPCglobal guidelines for RFID implementation.

But the proposed legislative notice was very specific. It would have established in law a requirement that the notice include a reference to a finding by that particular state government. It would have been economically infeasible to display such a notice but, more importantly, the notice invited every other jurisdiction to establish their own notice requirements or defer to the first state that acted, substituting speed to regulate for careful legislative review and action. Of course, it would be theoretically possible to manufacture different versions for each state but it would be akin to requiring a different cereal box for each state.

The uncertainty about varying legal and regulatory requirements has discouraged potential users of RFID technology. Investment has been delayed, deployment postponed, and research deferred.

Continuing uncertainty has had a chilling effect even given the demonstrable benefits of using the technology to improve efficiency, reduce costs, etc.

We offer this example not with a view that privacy issues are irrelevant or should not be addressed, but to emphasize the impact on innovation. One positive effect of the NOI would be a heightened focus on the need to harmonize or make interoperable differing policy frameworks regarding privacy.

VI. Information and Communications Technologies Operate Globally and Policies Must Be Harmonized to Reflect the Increasing Globalization of Both Commerce and Innovation

There are a number of useful precedents that demonstrate the means for and the beneficial results of policy harmonization. As an example, OECD accomplished foundational work in privacy through the development of its 1980 Privacy Guidelines. The Department's role in the development of the OECD guidelines and the 2005 Asia Pacific Economic Cooperation Privacy Framework provides a valuable legacy for the Department's present work in privacy.

The fact that the OECD's 1980's work—which predated the commercial internet, the explosive growth of e-commerce, and the emergence of broadband and mobile connectivity-- remains a foundation for today's privacy discussions is a testament not only to the thoughtfulness of the participants, but also to their focus on guiding principles and inclusive policy making processes.

The membership of the OECD and APEC consists of governments. Yet their privacy policymaking process brought together a wide variety of stakeholders including consumers, privacy advocates, academics, businesses in a mutually respectful environment where all interests could be examined. At the same time, the efforts did not seek detailed and prescriptive rules but guidelines that could be implemented in many different circumstances in countries with vastly differing legal systems and institutions. They recognized the importance of allowing policies and practices to emerge which could be evaluated in light of the guidelines and which could be reviewed and adapted as technologies and uses change over time. The guidelines were technologically neutral but the principles remained applicable whether the information was contained on paper records or in the sometimes evanescent digital "breadcrumbs" that may follow one's path on the World Wide Web.

In 2003, the GS1 EPCglobal entity created *Guidelines on EPC for Consumer Products* for the use of EPC-enabled RFID technology. EPCglobal brought together a large and disparate community involving a membership that comes from 108 different countries. Drawing upon Fair Information Practices, EPCglobal instituted a self-regulatory system to create an environment of trust for consumers and businesses. Based upon the collective experience of its membership it customized the privacy protections included in the Fair Information Practices to the particulars of the technology and its applications and established processes to review the *Guidelines* if significant changes in circumstances occur.

We believe that the Fair Information Practices have served us well. Notice (clear, accessible, comprehensible, and meaningful) and choice (effective, and easily implemented) will continue to be critical components of any long lasting privacy regime in part because notice and choice reflect the existence of rights and responsibilities for all parties to a potentially privacy affecting transaction. But the dramatic changes in our world reinforces the need for policymakers to step back, reconsider, and if necessary, amend present policies to better meet the challenges of the 21st century.

The NOI raises the possibility of a "use-based" model for privacy protection. At its core, we see the use-based model as reflecting an important insight—the parties most familiar with their plans and procedures should be incented to create and implement the most efficient and effective means of achieving well defined policy goals such as the protection of privacy. Defining the high level principles and setting any critical boundaries through rules of the road are by and large governmental functions, but decisions about their implementations in day to day processes and procedures should devolve to those closest to the specific facts with the strongest incentives to do things right.

VII. Connecting the Dots: Government's Expanding Data Collection

In Section 3, the Notice asked for comments on the impact of laws that permit governments to have access to personal information. While this question was posed in the context of international privacy laws and regulations, we believe that the issue applies to actions by governmental entities in the U.S. as well and is particularly timely.

One of the responses to the fears of global terrorism has been to dramatically increase the collection, sharing, and processing of information that might allow the government to anticipate and prevent terrorist acts. In today's dangerous world, intelligence and law enforcement officials are justifiably concerned with "connecting the dots". As is true with other privacy issues, this important effort to protect the national security raises potential conflicts with the protection of individual privacy. One fruitful area of investigation in constructing a privacy framework for the 21st century is the development of appropriate rules and procedures for government access to the vast amounts of data now being generated and collected in the private sector. Businesses everywhere would benefit from clear rules on what constitutes due process for government access to data in the face of challenges both domestic and foreign.

VIII. Privacy Enhancing Technologies and Aggregated Data

In Section 6, the NOI justifiably calls attention to the importance of privacy enhancing technologies and information management processes in the development of a 21st century privacy framework.

GS1 believes in the importance of developing these technologies and has been supporting related research at academic laboratories around the world.

We do believe, however, that government has an important role to play, particularly with respect to data de-identification and data re-identification.

Many of the great policy challenges facing our nation will depend on exploiting huge amounts of aggregated data. Just one example is comparative effectiveness research in healthcare. The ability to mine data from millions of de-identified/anonymized medical records to determine what medical treatments work and what treatments do not work is critical to increasing the effectiveness of medical interventions as well as controlling healthcare costs. Yet aggregating and mining such data, based upon sensitive medical records, poses real privacy risks, risks highlighted by recent research that shows the potential for re-identification of supposedly anonymized data.

In the past government has supported the creation of standards for the protection of information such as the digital encryption standard. This standard, the result of collaboration among the government's most sophisticated technical agencies, was adopted to protect governmental

information but was available for use by the U.S. private sector. Because creating an effective means of de-identifying large data sets presents substantial technical challenges and because the government would be a principle beneficiary of any successful de-identification effort, there is a strong argument for governmental support.

Creating a successful system for de-identification—long lasting, impervious to known challenges, easily and cost effectively implemented in a variety of settings without access to specialized expertise-- might be likened to the Grand Challenges that have helped spur technological development in areas such as the development of autonomous vehicles. Given the extraordinary benefits that appear to be achievable using aggregated data, de-identification deserves the Grand Challenge label and the associated governmental support.

One other comment should be made in connection to privacy enhancing technologies. It is well understood that corporations have an economic incentive to utilize data they generate to increase sales and profits. Corporations have economic incentives to protect privacy in order to develop strong bonds with their customers, providing more attractive goods and services, and to protect their brand equities, but these incentives could be strengthened. A new policy framework should examine the potential to increase the economic incentives for adoption of privacy enhancing technologies and further strengthening of privacy protections. There may be analogies in the example of using procurement policies to encourage smart building design or more sustainable computing devices that suggest new ways of using economic incentives to promote innovation in privacy protection by the private sector.

IX. Small and Medium-Sized Entities and Startup Companies

In Section 7, the Notice asks for comments on the impact of privacy laws on SME's.

As we noted over 200,000 companies, most of them SME's, participate in GS1 US. While they differ in many respects, they all depend on the confidence of their customers and have strong incentives to treat them in a way that they continue to be their customers. This clearly includes obeying laws and regulations regarding privacy.

A crucial difference between SMEs and larger commercial entities is their relative lack of resources for compliance with legal and regulatory requirements. In drafting the proposed PIA described in Section 5 above, we attempted to reduce, as much as possible the burden placed on the entity that is proposing a new RFID application. We would recommend as strongly as possible that evaluating the actual burden of compliance be a critical part of any privacy framework.

X. The Importance of Consumer Education

The role of government and the private sector in educating the public about privacy has received little attention. Yet in other areas of societal concern, preventing identity theft or reducing teen smoking, for example, public education has played a meaningful role. There do not appear to be similar efforts to help the public understand the increasing challenges they face regarding the protection of their personal privacy, the choices they have available, or ways they can make more informed decisions. Identifying the locus of such a public education effort and providing opportunities for the private sector to assist might have outsized benefits for its minimal costs.

XI. The Role of the Department of Commerce

We have the greatest respect for the efforts of the Federal Trade Commission, in particular, to protect consumer privacy. As can be seen in this Notice, however, the Department of Commerce brings an important and different perspective to discussions of privacy policy and innovation in a global context. We commend the Department's initiative and support its continued participation in the development of a privacy framework for the 21st century. We are pleased to be able to provide our comments in this important effort and stand ready to continue to support this process in whatever ways possible.

For more information, please contact:

Elizabeth Board
Executive Director, GS1 Global Public Policy
1101 30th St., NW Suite 500
Washington, DC 20007
elizabeth.board@gs1.org

www.DiscoverRFID.org
www.GS1US.org
www.GS1.org
www.EPCglobal.org
www.EPCglobalUS.org